SPLK-1003.28q

Number: SPLK-1003
Passing Score: 800
Time Limit: 120 min

SPLK-1003

Splunk Enterprise Certified Admin

Exam A

QUESTION 1
Which parent directory contains the configuration files in Splunk?

A. `$SPLUNK_HOME/etc`
B. `$SPLUNK_HOME/var`
C. `$SPLUNK_HOME/conf`
D. `$SPLUNK_HOME/default`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories

QUESTION 2
Which forwarder type can parse data prior to forwarding?

A. Universal forwarder
B. Heaviest forwarder
C. Hyper forwarder
D. Heavy forwarder

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders **QUESTION 3**
Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers
B. Forwarder
C. Search head
D. Search peers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Advancedindexingstrategy

QUESTION 4
Where should apps be located on the deployment server that the clients pull from?

A. `$SPLUNK_HOME/etc/apps`
B. `$SPLUNK_HOME/etc/search`
C. `$SPLUNK_HOME/etc/master-apps`
D. `$SPLUNK_HOME/etc/deployment-apps`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html

QUESTION 5
This file has been manually created on a universal forwarder:

`/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf`

```
[monitor:///var/log/messages]
sourcetype=syslog
index=syslog
```

A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new `inputs.conf` file: `/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf`

```
[monitor:///var/log/maillog]
sourcetype=maillog
index=syslog
```

Which file is now monitored?

A. `/var/log/messages`
B. `/var/log/maillog`
C. `/var/log/maillog` and `/var/log/messages`
D. none of the above

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation
B. Regular expression
C. Irregular expression
D. Wildcard-only expression

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients

QUESTION 7
What is required when adding a native user to Splunk? (Select all that apply.)

A. Password
B. Username
C. Full Name
D. Default app

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers

QUESTION 8
What are the minimum required settings when creating a network input in Splunk?

A. Protocol, port number
B. Protocol, port, location
C. Protocol, username, port
D. Protocol, IP, port number

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector

QUESTION 9
Which Splunk component requires a Forwarder license?

A. Search head
B. Heavy forwarder

C. Heaviest forwarder
D. Universal forwarder

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

QUESTION 10
Which optional configuration setting in `inputs.conf` allows you to selectively forward the data to specific indexer(s)?

A. `_TCP_ROUTING`
B. `_INDEXER_LIST`
C. `_INDEXER_GROUP`
D. `_INDEXER_ROUTING`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Monitorfilesanddirectorieswithinputs.conf

QUESTION 11
To set up a network input in Splunk, what needs to be specified?

A. File path.
B. Username and password.
C. Network protocol and port number.
D. Network protocol and MAC address.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

QUESTION 12
During search time, which directory of configuration files has the highest precedence?

A. `$SPLUNK_HOME/etc/system/local`
B. `$SPLUNK_HOME/etc/system/default`
C. `$SPLUNK_HOME/etc/apps/app1/local`
D. `$SPLUNK_HOME/etc/users/admin/local`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

QUESTION 13
Within `props.conf`, which stanzas are valid for data modification? (Select all that apply.)

A. Host
B. Server
C. Source
D. Sourcetype

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html

QUESTION 14
What is the correct order of steps in Duo Multifactor Authentication?

A. 1. Request Login
   2. Connect to SAML server
   3. Duo MFA
   4. Create User session
   5. Authentication Granted
   6. Log into Splunk

B. 1. Request Login
   2. Duo MFA
   3. Authentication Granted
   4. Connect to SAML server
   5. Log into Splunk
   6. Create User session

C. 1. Request Login
   2. Check authentication / group mapping
   3. Authentication Granted
   4. Duo MFA
   5. Create User session
   6. Log into Splunk

D. 1. Request Login
   2. Duo MFA
   3. Check authentication / group mapping
   4. Create User session
   5. Authentication Granted
   6. Log into Splunk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ConfigureDuo

QUESTION 15
Which of the following enables compression for universal forwarders in `outputs.conf`?

A. `[udpout:mysplunk_indexer11] compression=true`

B. `[tcpout] defaultGroup=my_indexers compressed=true`

C. `/opt/splunkforwarder/bin/splunk enable compression`

D. `[tcpount:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Outputsconf

QUESTION 16
User role inheritance allows what to be inherited from the parent role? (Select all that apply.)

A. Parents
B. Capabilities
C. Index access
D. Search history

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

QUESTION 17
Which of the following statements apply to directory inputs? (Select all that apply.)

A. All discovered text files are consumed.
B. Compressed files are ignored by default.
C. Splunk recursively traverses through the directory structure.
D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html

QUESTION 18
Which of the following is a valid distributed search group?

A.
```
[distributedSearch:Paris]
default = false servers =
server1, server2
```

B.
```
[searchGroup:Paris] default =
false
servers = server1:8089, server2:8089
```

C.
```
[searchGroup:Paris] default
= false
servers = server1:9997, server2:9997
```

D.
```
[distributedSearch:Paris]
default = false
servers = server1:8089; server2:8089
```

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Distributedsearchgroups

QUESTION 19
Local user accounts created in Splunk store passwords in which file?

A. `$SPLUNK_HOME/etc/passwd`
B. `$SPLUNK_HOME/etc/authentication`
C. `$SPLUNK_HOME/etc/users/passwd.conf`
D. `$SPLUNK_HOME/etc/users/authentication.conf`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

QUESTION 20
For single line event sourcetypes, it is most efficient to set `SHOULD_LINEMERGE` to what value?

A. True
B. False
C. <regex string> D. Newline Character

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

QUESTION 21
Which Splunk component does a search head primarily communicate with?

A. Indexer
B. Forwarder
C. Cluster master
D. Deployment server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

QUESTION 22
Which layers are involved in Splunk configuration file layering? (Select all that apply.)

A. App context
B. User context
C. Global context
D. Forwarder context

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Wheretofindtheconfigurationfiles **QUESTION 23**
Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform.
B. Linux platform only.
C. Windows platform only.
D. None of the above.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
What are the required stanza attributes when configuring the `transforms.conf` to manipulate or remove events?

A. REGEX, DEST, FORMAT
B. REGEX, SRC_KEY, FORMAT
C. REGEX, DEST_KEY, FORMAT
D. REGEX, DEST_KEY, FORMATTING

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Transformsconf

QUESTION 25
Which of the following indexes come pre-configured with Splunk Enterprise? (Select all that apply.)

A. _licence
B. _internal
C. _external
D. _thefishbucket

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howindexingworks

QUESTION 26
How often does Splunk recheck the LDAP server?

A. Every 5 minutes.
B. Each time a user logs in.
C. Each time Splunk is restarted.
D. Varies based on LDAP_refresh setting.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://docshare02.docshare.tips/files/22651/226514302.pdf

QUESTION 27
In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.
B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.
C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.
D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html

QUESTION 28
Which Splunk component performs indexing and responds to search requests from the search head?

A. Forwarder
B. Search peer
C. License master
D. Search head cluster

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.edureka.co/blog/splunk-architecture/

https://vceplus.com/